Endpoint based Micro-Segmentation

Implementing 'Next-Generation' Network Attack Protection

Version 1.0

Authors:
Donny Maasland, Chief Research Officer - ESET Netherlands
Jamil Sosa, Support Engineer - ESET Netherlands
Michael van der Vaart, Chief Technology Officer - ESET Netherlands

ENJOY SAFER TECHNOLOGY™

Introduction

Recent years have shown a notable shift in the TTPs (Tactics, Techniques and Procedures) of cybercriminals. Where specific data or systems used to be the direct targets of attacks, it is becoming steadily more common for attackers to first gain limited access (a foothold) to a network, and then to use 'lateral movement' to gain access to other systems within the same network, until the final objective has been reached. Recent examples of these methods are the attacks with malware such as 'WannaCry,' 'NotPetya' and 'BadRabbit'.

In these attacks it was notable that it were not server systems, but (legitimate software on) workstations which were largely being used to carry out the attack. This white paper has been written with the intention of protecting all systems within the network to the fullest against such attacks, using a whitelist principle.

Defense in depth & multi-layered security

ESET's security solutions have been developed over more than 30 years using the 'defense in depth' principle. Thus the most recent version of ESET Endpoint Security offers not just traditional protection techniques, but also Next-Gen methods like Machine Learning, Artificial Intelligence and the power of the Cloud. These techniques are also used not just to protect the local system, but are in fact fully integrated in the Network Attack Protection module for instance, where the system is protected continuously against network-based attacks. The combination of these techniques and modules offers an optimized and intelligent method of protection in almost all situations, while still giving managers and security specialists the required controls to raise the security maturity level to new heights.

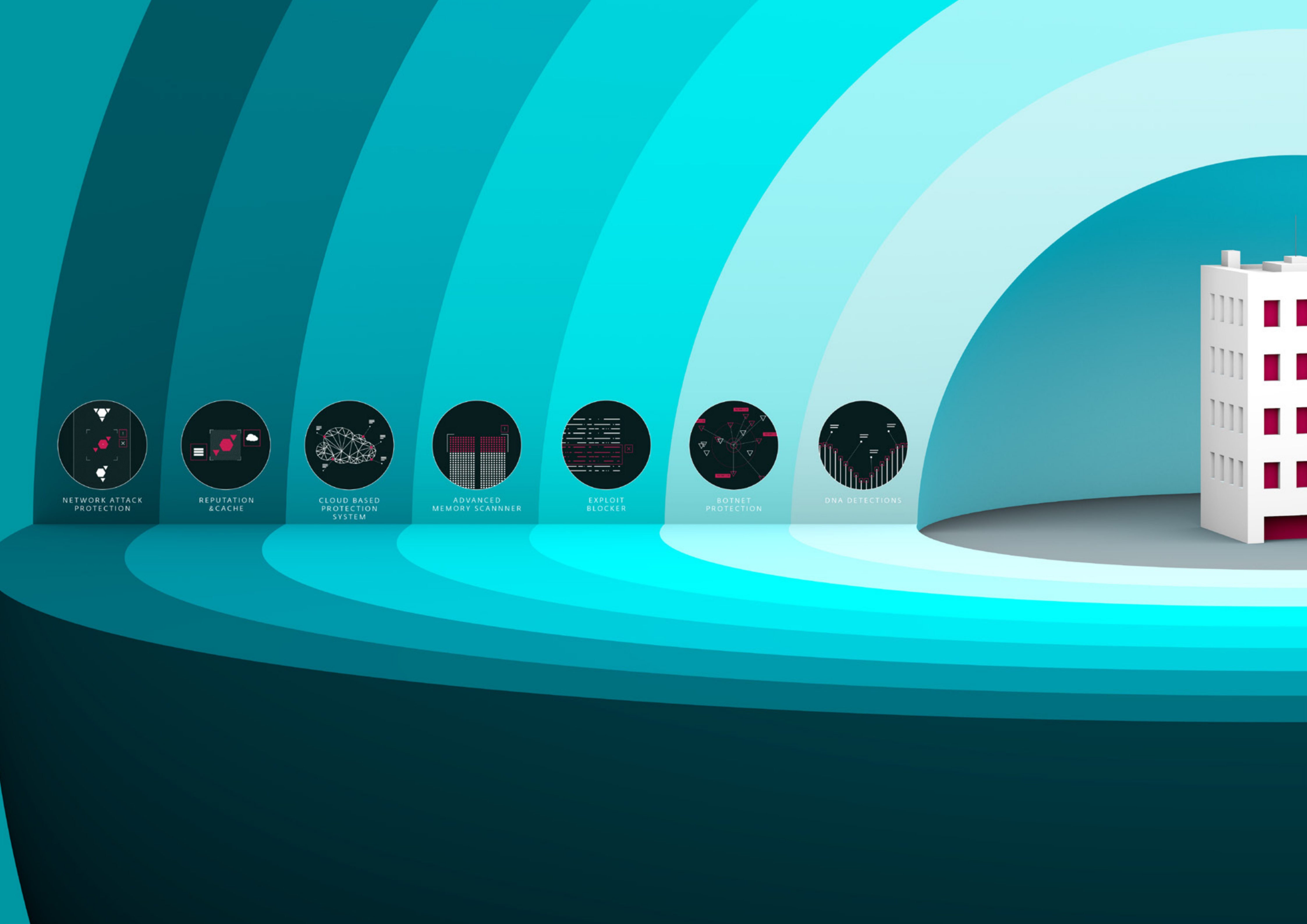
Important: NAP is part of ESET Endpoint Security.

Endpoint based Micro-Segmentation

This tech brief can be used to configure the Network Attack Protection module on the endpoints in the network to work in accordance with the 'whitelist' principle. In other words, the system only grants access to network services like Remote Desktop (RDP), Server Message Block (SMB), Windows Management Instrumentation (WMI) and Remote Procedure Call (RPC) interfaces to approved systems within the network. This whitelist is referred to in the ESET security solutions as the Trusted Zone. For systems which are not located in the Trusted Zone, an endpoint will not even be invisible within the network.

Make lateral movement impossible

The result of this configuration is that each endpoint is located in a closed 'micro-segment', and can only communicate with systems specified in the Trusted Zone. In practice this means that when one of the endpoints is successfully compromised by an attacker, it is impossible to compromise other endpoints through lateral movement and thereby gain a better foothold in the network, or spread malware further in the network.


NETWORK ATTACK PROTECTION
REPUTATION &CACHE
CLOUD BASED PROTECTION SYSTEM
ADVANCED MEMORY SCANNNER
EXPLOIT BLOCKER
BOTNET PROTECTION
DNA DETECTIONS

Implementation of Endpoint Micro-Segmentation

In global terms, implementation of the configuration mentioned above comprises two steps:

- Install and configure the 'ESET Authentication Server'
- Configure the endpoints with the 'ESET Remote Administrator'

This manual assumes there is a working ESET Remote Administrator within the network.

ESET Authentication Server

The ESET Authentication Server is a cost-free program which makes it possible to authenticate and verify a network based on 'Public-key Cryptography'. Installing and configuring the ESET Authentication Server is outside the scope of this white paper, but is described in detail in the following article: https://support.eset.com/KB2501/.

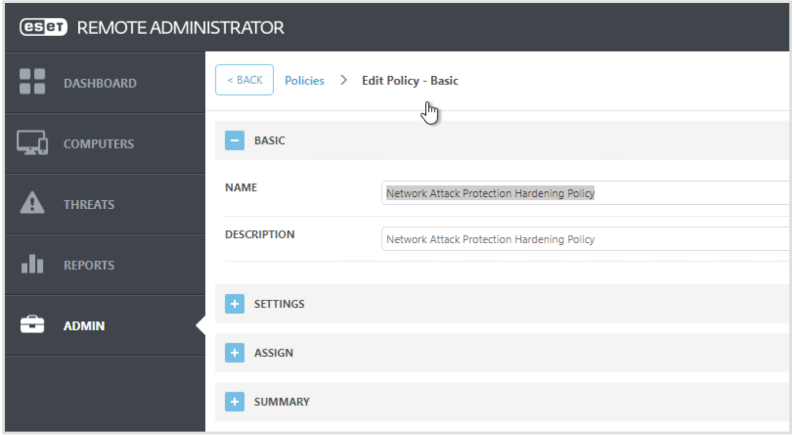
Important: make a note of the chosen 'Zone name' when configuring the ESET Authentication Server. This will be needed for configuring the endpoints.

Endpoint Configuratie

In this white paper, the endpoints will be configured using a 'Policy' with the help of the ESET Remote Administrator. If this procedure is either partially or fully unfamiliar, more information can be obtained from the following article: https://support.eset.com/KB3594/.

Step 1

To configure the endpoints, create a new policy and choose a suitable name for it, e.g. 'Network Attack Protection Hardening'.



NAME: Network Attack Protection Hardening Policy

DESCRIPTION: Network Attack Protection Hardening Policy

Useful to know!
Flags determine how a setting is handled by the policy. You can select one of the following flags for each setting:

○ Not applicable – Every setting with this flag is not set by policy. Because the setting is not enforced, it can be changed later by other policy lines.

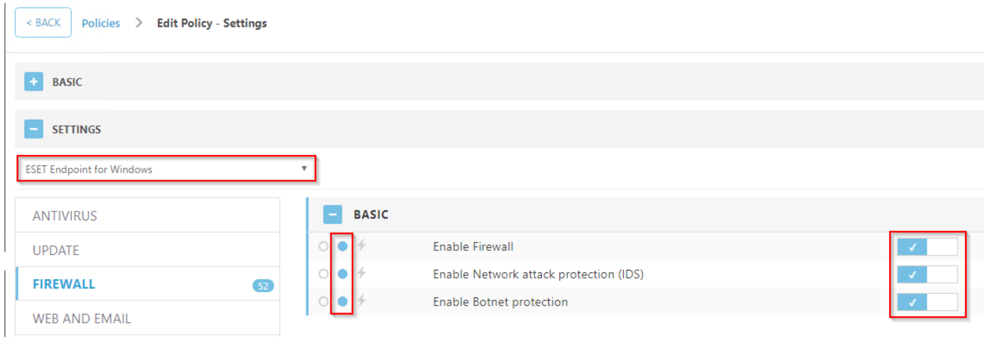
● Apply – Settings with this flag are sent to the client. However if policies are combined this can be overwritten by a later policy. If a policy is applied on a client computer and a particular setting has this flag, this setting is changed irrespective of what is configured locally on the client. Because the setting is not enforced, it can be changed later by other policy lines.

⚡ Force – Settings with the Force flag take priority and cannot be overwritten by a later policy (even if that later policy contains a Force flag). This ensures that this setting will not be changed by later policy during merging.

Stap 2

Under 'Settings' choose 'ESET Endpoint for Windows' as product, and then click 'Personal Firewall'. In the 'BASIC' section set the following options:

- Enable Firewall
- Enable Network Attack Protection (IDS)
- Enable Botnet Protection



< BACK · Policies > Edit Policy - Settings

BASIC

SETTINGS

ESET Endpoint for Windows

BASIC

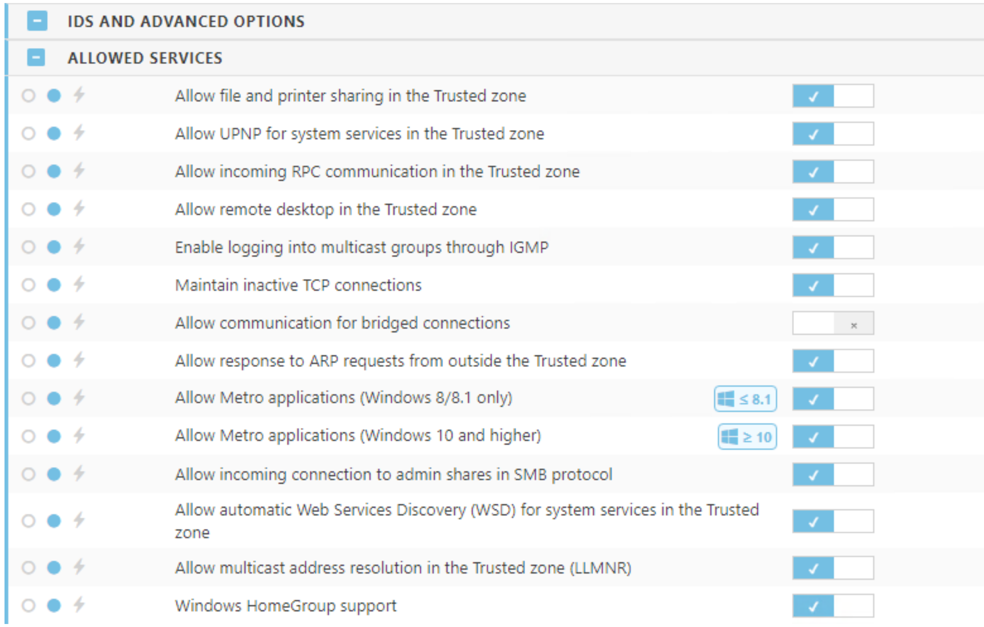
Setting	
Enable Firewall	✓
Enable Network attack protection (IDS)	✓
Enable Botnet protection	✓

Stap 3

Then navigate to 'ADVANCED' -> 'IDS AND ADVANCED OPTIONS', and copy the configuration as shown, which will offer a solid basic configuration. It's advisable to check which options may need to be configured differently for the optimum protection of the environment in question. More background information about (one of) the settings can be found on the following page:

https://help.eset.com/ees/6/en-US/idh_config_epfw_advanced_settings.htm?zoom_highlightsub=ids+options

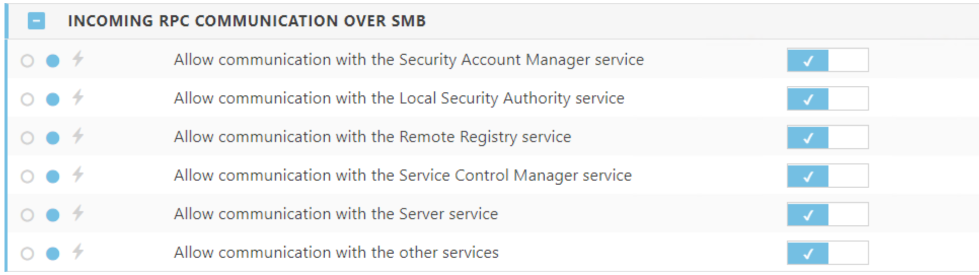
IMPORTANT
The availability of various options in this window can vary and depends on the type or the version of your ESET product and module for the firewall, but also on your operating system version.



IDS AND ADVANCED OPTIONS

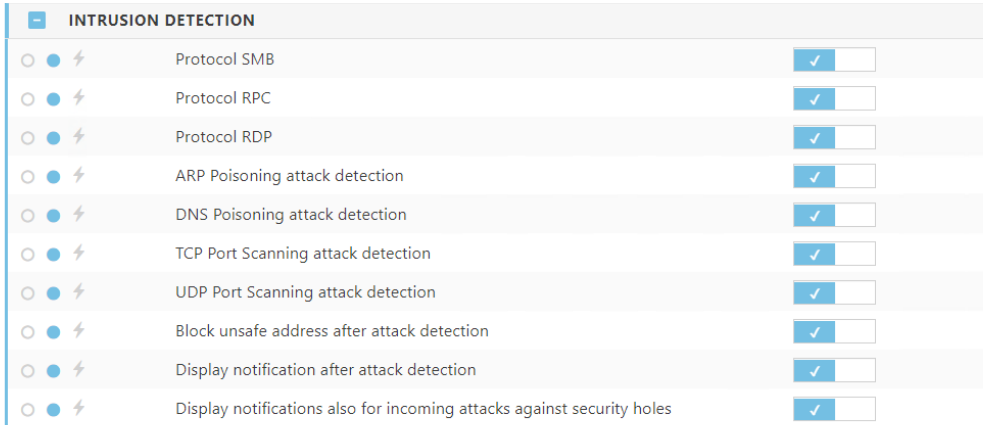
ALLOWED SERVICES

Setting	
Allow file and printer sharing in the Trusted zone	✓
Allow UPNP for system services in the Trusted zone	✓
Allow incoming RPC communication in the Trusted zone	✓
Allow remote desktop in the Trusted zone	✓
Enable logging into multicast groups through IGMP	✓
Maintain inactive TCP connections	✓
Allow communication for bridged connections	×
Allow response to ARP requests from outside the Trusted zone	✓
Allow Metro applications (Windows 8/8.1 only) ≤ 8.1	✓
Allow Metro applications (Windows 10 and higher) ≥ 10	✓
Allow incoming connection to admin shares in SMB protocol	✓
Allow automatic Web Services Discovery (WSD) for system services in the Trusted zone	✓
Allow multicast address resolution in the Trusted zone (LLMNR)	✓
Windows HomeGroup support	✓



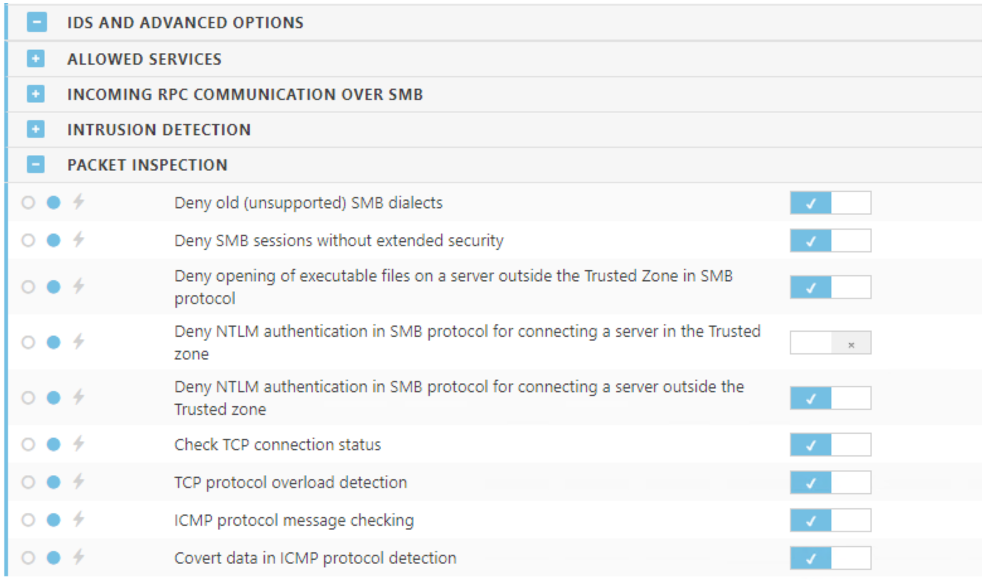
INCOMING RPC COMMUNICATION OVER SMB

Setting	
Allow communication with the Security Account Manager service	✓
Allow communication with the Local Security Authority service	✓
Allow communication with the Remote Registry service	✓
Allow communication with the Service Control Manager service	✓
Allow communication with the Server service	✓
Allow communication with the other services	✓



INTRUSION DETECTION

Protocol SMB	✓
Protocol RPC	✓
Protocol RDP	✓
ARP Poisoning attack detection	✓
DNS Poisoning attack detection	✓
TCP Port Scanning attack detection	✓
UDP Port Scanning attack detection	✓
Block unsafe address after attack detection	✓
Display notification after attack detection	✓
Display notifications also for incoming attacks against security holes	✓



IDS AND ADVANCED OPTIONS

ALLOWED SERVICES

INCOMING RPC COMMUNICATION OVER SMB

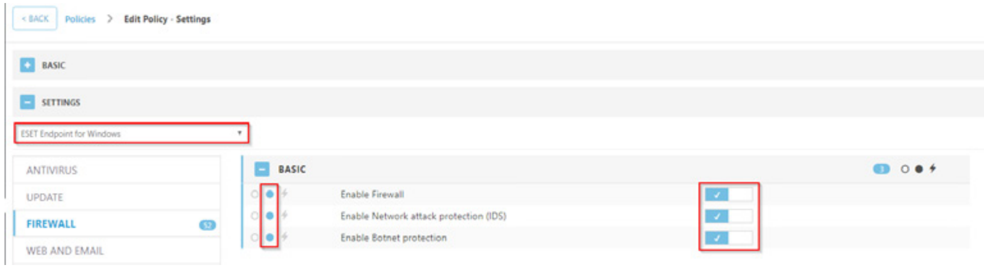
INTRUSION DETECTION

PACKET INSPECTION

Deny old (unsupported) SMB dialects	✓
Deny SMB sessions without extended security	✓
Deny opening of executable files on a server outside the Trusted Zone in SMB protocol	✓
Deny NTLM authentication in SMB protocol for connecting a server in the Trusted zone	×
Deny NTLM authentication in SMB protocol for connecting a server outside the Trusted zone	✓
Check TCP connection status	✓
TCP protocol overload detection	✓
ICMP protocol message checking	✓
Covert data in ICMP protocol detection	✓

Stap 4

Then navigate to 'KNOWN NETWORKS'. Here select 'Mark as public' for the 'Protection type of new networks' option. Then enable 'Do not ask for protection type of new networks. Automatically mark new networks as public'. Then click 'Edit' at 'Known networks'.

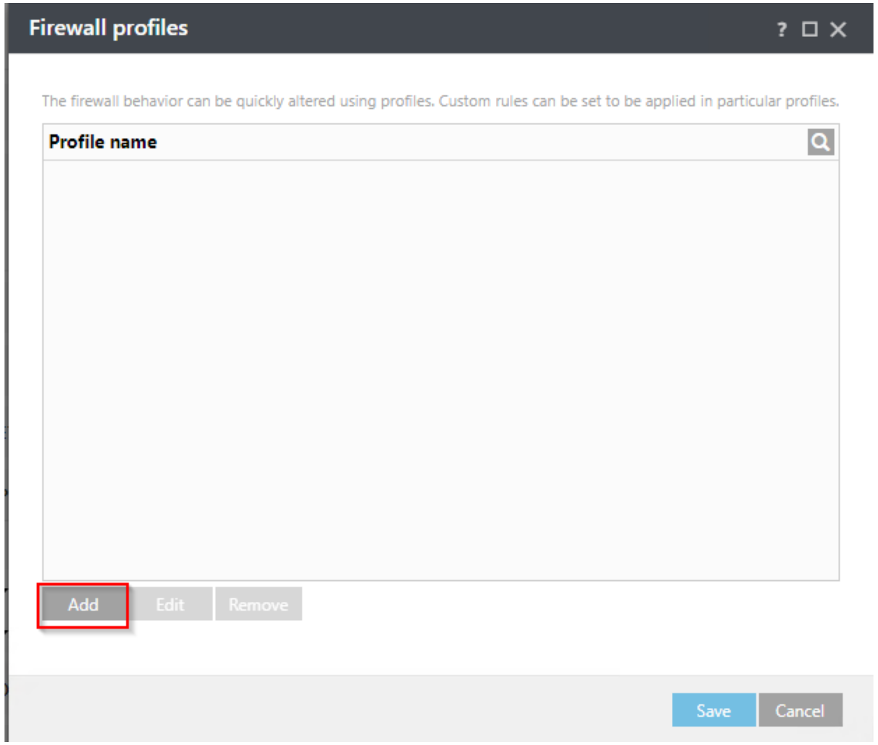


ESET Endpoint for Windows

Enable Firewall	✓
Enable Network attack protection (IDS)	✓
Enable Botnet protection	✓

Click "Add" in the window that opens and configure the following options:

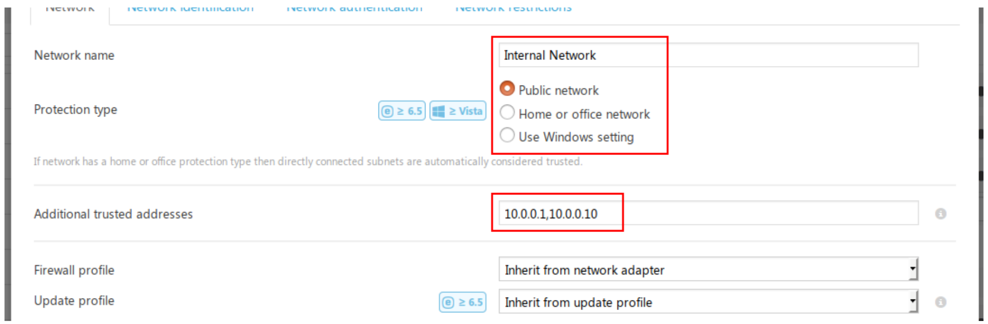
- **Network name**: Internal Network (**IMPORTANT**: Choose the same name here as for the "Zone name" that was selected during the configuration of the ESET Authentication Server.)
- **Protection Type**: Public network
- **Additional trusted addresses**: Enter the systems here that are allowed to connect to the network services of the endpoints. For example, consider the Domain Controller, SCCM server or generic management server. Note that you keep the number of addresses as low as possible.
- **(Optioneel) Firewall Profile**: a firewall profile that only applies to this zone.
- **(Optioneel) Update Profile**: an update profile that only applies to this zone.



Firewall profiles

The firewall behavior can be quickly altered using profiles. Custom rules can be set to be applied in particular profiles.

Profile name



Network name: Internal Network

Protection type: ● Public network ○ Home or office network ○ Use Windows setting

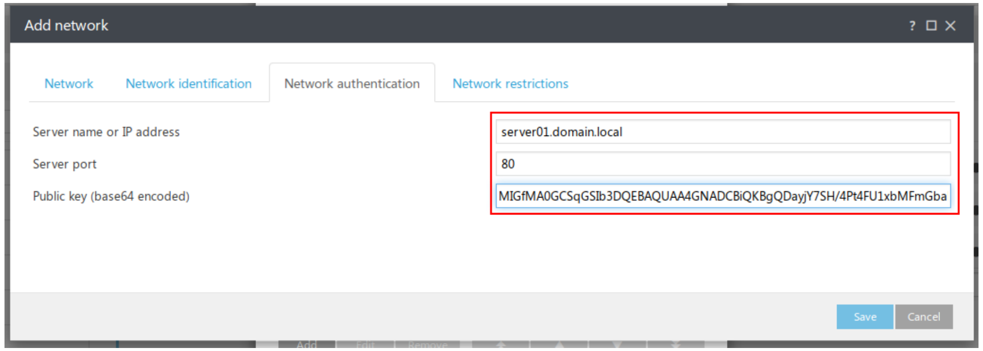
If network has a home or office protection type then directly connected subnets are automatically considered trusted.

Additional trusted addresses: 10.0.0.1,10.0.0.10

Firewall profile: Inherit from network adapter

Update profile: Inherit from update profile

Then click the 'Network Authentication' heading and enter the details of the ESET Authentication Server.



Add network

Server name or IP address: server01.domain.local

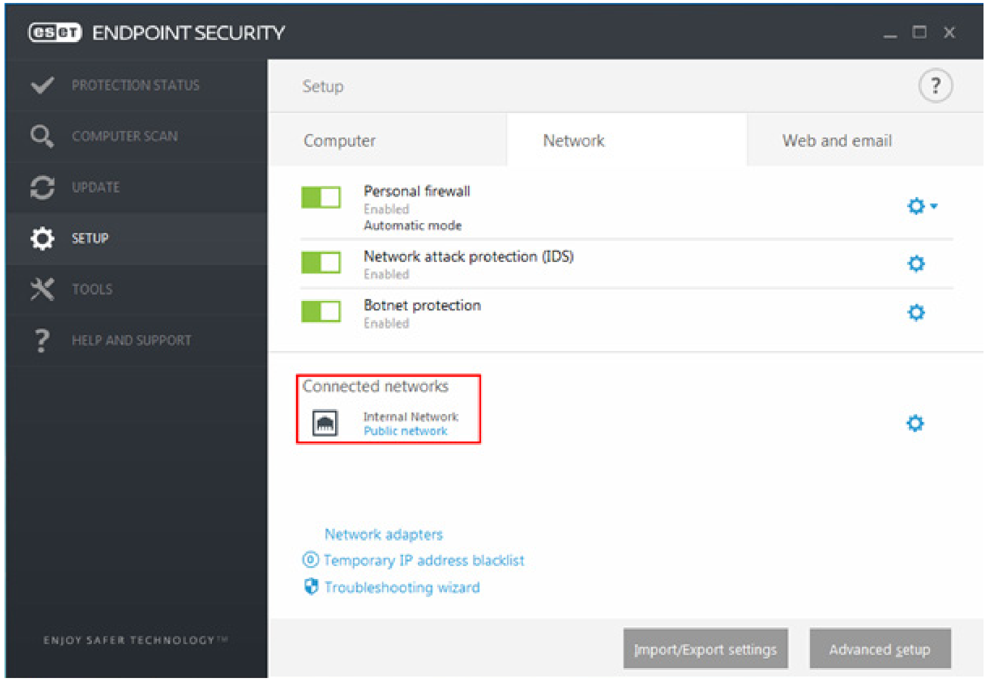
Server port: 80

Public key (base64 encoded): MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDayjY7SH/4Pt4FU1xbMFmGba

Then click 'Save' twice. Expand the 'ASSIGN' section and click 'ASSIGN...'. In the window that opens, select which systems the Policy applies to. Then click 'Finish'.

Stap 5

Once the configuration has been completed successfully, the endpoints can be checked to see whether the settings are correct, by navigating to 'Setup -> Network'. Check under 'Connected Networks' whether the entered network is named, and that 'Protection Type' is on 'Public Network'.



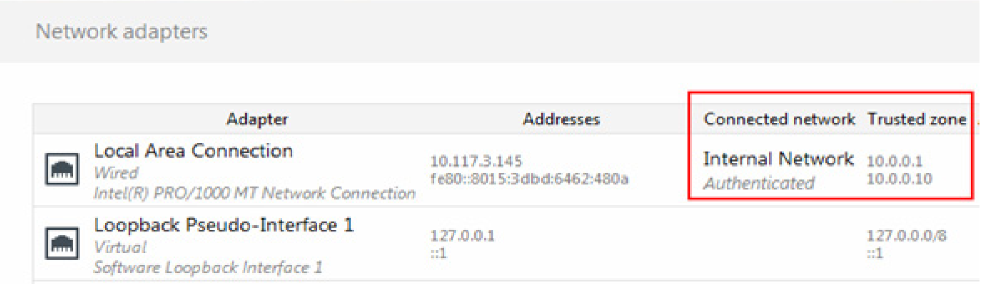
Personal firewall
Enabled
Automatic mode

Network attack protection (IDS)
Enabled

Botnet protection
Enabled

Connected networks
Internal Network
Public network

Then click 'Network Adapters' and check whether the Trusted Zone has been applied correctly, and whether the word 'Authenticated' is shown under the heading 'Connected Network'.



Network adapters

Adapter	Addresses	Connected network	Trusted zone
Local Area Connection *Wired* *Intel(R) PRO/1000 MT Network Connection*	10.117.3.145 fe80::8015:3dbd:6462:480a	Internal Network *Authenticated*	10.0.0.1 10.0.0.10
Loopback Pseudo-Interface 1 *Virtual* *Software Loopback Interface 1*	127.0.0.1 ::1		127.0.0.0/8 ::1

If this is the case, the endpoint will grant addresses in the Trusted Zone access to the available network services, if it is able to authenticate the network successfully with the ESET Authentication Server. If the authentication fails, or if the ESET Authentication Server cannot be reached, the Trusted Zone will remain empty and absolutely no system will be able to connect with the endpoint.

Tot slot

By copying the configuration as described in this white paper, the security maturity level of the organization will be raised to a higher level. However it is advisable to look critically at the available options of the ESET Endpoint software to tailor the configuration more towards the organization.

Thus for instance firewall profiles could be used to ensure that an endpoint outside the internal network can only make a VPN connection with the organization before further network traffic is permitted, or Address Resolution Protocol (ARP) traffic from outside the Trusted Zone can even be blocked, whereby the endpoint at layer 2 of the OSI model becomes invisible to other endpoints.

ESET technology is continuously being developed and therefore this tech brief will be updated to modern developments.

Contactgegevens

ESET Business Support
support@eset.nl
+31 (0)184 647745